IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

BONITA ODELL, individually and on behalf of all others similarly situated, Plaintiff, v. U.S. VISION, INC., USV OPTICAL, INC., and NATIONWIDE OPTOMETRY, P.C., Defendants.	Case No. **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Bonita Odell, individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants U.S. Vision, Inc. ("U.S. Vision"), USV Optical, Inc. ("USV"), and Nationwide Optometry, P.C. ("Nationwide") (collectively "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard her and approximately 711,072 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, Social Security numbers, taxpayer identification numbers, driver's license or state identification numbers, financial account information, medical and/or treatment information, health insurance information, billing and claims information, biometric data, email addresses, usernames, and passwords.

2. U.S. Vision is a company that provides eyecare services and sells eyecare products. U.S. Vision's principal office is located in Blackwood, New Jersey.

3. USV is a subsidiary of U.S. Vision. It is incorporated in Texas, with its principal place of business located in Blackwood, New Jersey.

4. Nationwide is an eyecare service provider. Nationwide's principal place of business is located in Chandler, Arizona.

5. Between April 20, 2021 and May 17, 2021, an unauthorized individual, or unauthorized individuals, gained access to U.S. Vision's network systems and accessed and acquired files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

6. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients' PII/PHI from unauthorized access and disclosure.

7. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which U.S. Vision says it learned of on or about May 12, 2021.

8. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the Arizona Consumer Fraud Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

9. Plaintiff Bonita Odell is an Arizona resident. From approximately 2019 to 2020, she obtained eyecare services from Nationwide. She received a letter from Nationwide in or about October of 2022, which notified her that her PII/PHI was accessed in the Data Breach. Plaintiff Odell would not have sought services from or provided her PII/PHI to Nationwide had she known that her information would not be adequately safeguarded by Defendants. As a result of the Data Breach, Plaintiff Odell has suffered a dramatic increase in the number of spam telephone calls she receives. Since the Data Breach, these spam calls have become a constant source of frustration for her and her family.

10. Defendant U.S. Vision, Inc. is a Delaware corporation with its principal place of business in Blackwood, New Jersey. U.S. Vision's headquarters are located at 1 Harmon Drive, Blackwood, New Jersey 08012. U.S. Vision may be served through its registered agent: Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

11. Defendant USV Optical, Inc. is a Texas corporation with its principal place of business in Blackwood, New Jersey. USV's headquarters are located at 1 Harmon Drive, Blackwood, New Jersey 08012. USV may be served through its registered agent: Corporation Service Company, d/b/a CSC Lawyers Incorporated, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

12. Defendant Nationwide Optometry, P.C. is a professional corporation formed in Arizona. Nationwide's principal place of business is 220 North McKemy Avenue, Chandler, Arizona 85226. Nationwide may be served through its registered agent: C T Corporation System, 38900 North Central Avenue, Suite 460, Phoenix, Arizona 85012.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from the citizenship of all of Defendants' members, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

14. This Court has personal jurisdiction over U.S. Vision, Inc. and USV Optical, Inc. because U.S. Vision, Inc. and USV Optical, Inc. have their principal place of business in New Jersey.

15. This Court has personal jurisdiction over Nationwide Optometry, P.C. because Nationwide contracted with U.S. Vision, which has its principal place of business in New Jersey, and shared Plaintiff's PII/PHI with U.S. Vision in New Jersey.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because U.S. Vision, Inc. and USV Optical, Inc.'s principal place of business is in New Jersey; Nationwide Optometry P.C. does business with U.S. Vision, Inc. in this District; and a significant amount of the events leading to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

17. U.S. Vision "is a retailer of optical products and services."[1] U.S. Vision "provide[s] a wide variety of services including comprehensive eye exams, contact lens fittings, and [prescription] updates."[2] In the regular course of its business, U.S. Vision collects and maintains the PII/PHI of its patients and its affiliates' patients.

[1] *Homepage*, U.S. VISION, https://www.usvision.com/ (last accessed Nov. 21, 2022).
[2] *About U.S. Vision*, U.S. VISION, https://www.usvision.com/about-us/ (last accessed Nov. 21, 2022).

18. USV is a subsidiary of U.S. Vision.[3]

19. Nationwide "provides complete eye care services," including care relating to "routine exams, glasses, [and] contact lenses."[4] Nationwide also provides services for cataracts, glaucoma, macular degeneration, and pterygium treatment.[5]

20. Nationwide's website contains a Privacy Policy which states, "[Nationwide] takes the privacy of its users' . . . information very seriously."[6] The Policy goes on to state that Nationwide will not share its patients' personal information except in enumerated circumstances.[7] The Policy also states, "We are required by applicable law to maintain the privacy of your health information."[8] The Policy further states, "We follow generally accepted industry standards to protect the personal information submitted to us, and to protect against loss, misuse or alteration of your information."[9]

21. The Privacy Policy also provides:

> Unless otherwise provided in this Privacy Policy, we shall not disclose Personal Information you submit to us except (i) with affiliates, licensees, subsidiaries and successors, (ii) when we have your permission, or (iii) as necessary to:
>
> - To our affiliates as permitted by law;
> - To third parties who provide information technology services such as website hosting, computer systems maintenance, or data security and privacy services;
> - To our partners, vendors or others who help us operate the Services or assess your interest or satisfaction with the Services, our organization, or our products, provided they have contractually agreed to adhere to this Privacy Policy; or

---

[3] Notice of Data Security Incident, NATIONWIDE, https://response.idx.us/incident-information/ (last accessed Nov. 21, 2022).
[4] *Nationwide Vision Eye Care Services in Arizona*, Nationwide Vision, https://www.nationwidevision.com/eye-care-services (last accessed Nov. 21, 2022).
[5] *See id.*
[6] *Privacy Policy*, Nationwide Vision, https://www.nationwidevision.com/privacy-policy (last accessed Nov. 21, 2022).
[7] *See id.*
[8] *Id.*
[9] *Id.*

- To comply with our legal obligations, enforce this Privacy Policy, any other [Nationwide] agreements, or otherwise to protect the rights, property or safety of our users and business partners.[10]

The Privacy Policy even promises that Nationwide "follow[s] generally accepted industry standards to protect the personal information submitted to us, and to protect against loss, misuse or alteration of your information."[11]

22. Plaintiff and Class members are, or were, patients of Defendants and entrusted Defendants with their PII/PHI.

The Data Breach

23. Between April 20, 2021 and May 17, 2021, an unauthorized individual, or unauthorized individuals, gained access to U.S. Vision's network systems and accessed and acquired certain files on U.S. Vision's computer systems.

24. The Data Breach impacted current and former patients of U.S. Vision, Nationwide, as well as Sightcare, Inc., an Arizona eyecare provider.[12]

25. U.S. Vision notified Nationwide about the Data Breach on May 12, 2021. The notice that Nationwide posted to its website states that the information that the cybercriminal had access to includes the following PII/PHI:

> (1) identifying information (such as full name, date of birth, and address); (2) Social Security number, taxpayer identification number, driver's license or state identification number, and/or financial account information; (3) medical and/or treatment information (such as medical record number, dates of service, provider name, diagnosis or symptom information, and prescription/medication); (4) health insurance information (such as payor and subscriber/Medicare/Medicaid number); and (5) billing and claims information . . . . For a limited number of individuals, biometric data and/or email address or username and password were also included in the affected data.[13]

---

[10] *Id.*
[11] *Id.*
[12] *See Notice of Data Security Incident*, *supra* note 4.
[13] *Id.*

26. Defendants' notice states that their investigation into the Data Breach revealed that "files containing [patients'] information may have been viewed and/or taken by the unauthorized individual."[14]

Defendants Knew that Criminals Target PII/PHI

27. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks that Defendants should have anticipated and guarded against.

28. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[15]

29. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021 with over 50 million patient records exposed.[16] This is an

[14] *Id*.
[15] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[16] *See* PROTENUS, *2022 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Nov. 21, 2022).

increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[17]

30. PII/PHI is a valuable property right.[18] The value of PII/PHI as a commodity is measurable.[19] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[20] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[21] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

31. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

---

[17] *See id*.
[18] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[19] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[20] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[21] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

32. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[22] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[23]

33. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[24] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[25]

34. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[26] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[27]

---

[22] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[23] *Id.*

[24] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[25] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Nov. 21, 2022).

[26] *What Happens to Stolen Healthcare Data*, *supra* n.22.

[27] *Id.*

35. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

36. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

37. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[29]

38. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[30] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is

[28] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[29] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 21, 2022).

[30] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[31]

39. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.[32]

40. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[33]

41. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[31] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Nov. 21, 2022).

[32] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 21, 2022).

[33] *See* Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 21, 2022).

42. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[34]

43. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[35] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[36] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [37] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[38]

44. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified

[34] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[35] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[36] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* n.26.
[37] *See What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 14, 2022).
[38] *Id*.

information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[39]

45. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[40]

46. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of

[39] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* n.35.
[40] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

47. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

48. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

49. Plaintiff brings this action on behalf of herself and all members of the following Nationwide Class of similarly situated persons:

> All persons whose personally identifiable information or personal health information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

50. Excluded from the Class are U.S. Vision, Inc., USV Optical, Inc., Nationwide Optometry, P.C., and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

51. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

52. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Defendants reported to the United States Department of Health and Human Services Office of Civil Rights that approximately 711,072 persons' information was exposed in the Data Breach.

53. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

g. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

54. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

55. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

56. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

57. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class

members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding, securing, and protecting the PII/PHI in their possession, custody, or control.

60. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that have targeted companies that stored PII/PHI in recent years.

61. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

62. Nationwide explicitly promises in its Privacy Policy to follow industry standards and use reasonable methods to protect the PII/PHI in its control.

63. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

64. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants' possession.

65. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

66. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, adopting, implementing, and maintaining appropriate security measures.

67. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts

attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

68. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

69. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

70. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII/PHI.

71. Defendants violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtain and store, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

72. Defendants' violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

73. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

74. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

75. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

76. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' violations of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences

of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

77. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

78. As a condition of obtaining services from Defendants, Plaintiff and Class members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

79. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected.

80. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise,

publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

81. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

82. In connection with receiving health care services, Plaintiff and all other Class members entered into implied contracts with Defendants.

83. Pursuant to these implied contracts, Plaintiff and Class members paid money to Defendants and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (1) provide eyecare services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

84. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Nationwide recognized the importance of data security and the privacy of its patients' PII/PHI in its Privacy Policy. Had Plaintiff and Class members known that

Defendants would not adequately protect their patients' and former patients' PII/PHI, they would not have paid for eyecare services from Defendants.

85. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for eyecare services from Defendants.

86. Defendants breached their obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

87. Defendants' breach of their obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

88. Plaintiff and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will

continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

89. Plaintiff realleges and incorporates by reference paragraphs 1–80 as if fully set forth herein.

90. This claim is pleaded in the alternative to the breach of implied contract claim.

91. In obtaining services from Defendants, Plaintiff and Class members provided and entrusted their PII and PHI to Defendants.

92. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for eyecare services.

93. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services.

94. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

95. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

96. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *et seq*. ("ACFA")

97. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

98. The ACFA states:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

A.R.S. § 44-1522(A).

99. Plaintiff, Class members, and Defendants are "persons" under the ACFA. A.R.S. § 44-1521(6).

100. The services that Defendants provide are "merchandise" pursuant to the ACFA. A.R.S. § 44-1521(5).

101. Defendants make representations to their patients that their PII/PHI will remain private, as evidenced by, *inter alia*, Nationwide's Privacy Policy.

102. Defendants engaged in unlawful practices in violation of the ACFA by failing to implement and maintain reasonable security measures to protect and secure their patients' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards and failing to inform Plaintiff and Class members that they would not adequately secure their PII/PHI.

103. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding their patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

104. Plaintiff and all other Class members were damaged by Defendants' violation of the ACFA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 23, 2022

Respectfully submitted,

/s/ Janine Pollack
Janine Pollack
CALCATERRA POLLACK LLP
1140 Avenue of the Americas, 9th Floor
New York, New York 10036
Phone: (212) 899-1760
Fax: (332) 206-2073
Email: jpollack@calcaterrapollack.com

Ben Barnow*
Anthony L. Parkhill*
Riley W. Prince*
Barnow and Associates, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com

Counsel for Plaintiff Bonita Odell

* *Pro hac vice forthcoming*